

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION

SUSAN CLEMENTS-JEFFREY, et al.,	:	
	:	
Plaintiffs,	:	Case No. 3:09-cv-84
	:	
vs.	:	
	:	JUDGE WALTER HERBERT RICE
CITY OF SPRINGFIELD, OHIO, et al.,	:	
	:	
Defendants	:	

DECISION AND ENTRY SUSTAINING MOTION FOR PARTIAL SUMMARY JUDGMENT OF DEFENDANTS CITY OF SPRINGFIELD, GEOFFREY ASHWORTH AND NOEL LOPEZ (DOC. #70); OVERRULING DEFENDANTS ABSOLUTE SOFTWARE, INC.'S AND KYLE MAGNUS' MOTION FOR SUMMARY JUDGMENT (DOC. #78)

Plaintiffs Susan Clements-Jeffrey and Carlton Smith filed suit against The City of Springfield, Springfield police officers Geoffrey Ashworth and Noel Lopez (collectively “the Springfield Defendants”), Absolute Software, Inc. (“Absolute”), and Absolute’s theft recovery officer, Kyle Magnus (collectively “the Absolute Defendants”). In Count I of the Third Amended Complaint, Plaintiffs seek relief under 42 U.S.C. § 1983 against Ashworth and Lopez, alleging violations of the Fourth and Fourteenth Amendments. In Count II, Plaintiffs allege that Defendants violated the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2511, and the Stored Communications Act (“SCA”), 18 U.S.C. § 2701. In Count III, Plaintiffs allege that Ashworth, Lopez, Magnus, and Absolute intentionally invaded

their privacy.

This matter is currently before the Court on the Springfield Defendants' Motion for Partial Summary Judgment (Doc. #70), and the Absolute Defendants' Motion for Summary Judgment (Doc. #78).<sup>1</sup>

#### **I. Background and Procedural History<sup>2</sup>**

The Clark County School District purchased laptop computers, one of which was issued to a vocational student, Dusty Ray Powell. On April 9, 2008, when Powell was at the Springfield Public Library, someone stole that laptop. That same day, Powell reported the theft to the City of Springfield Police Department. Parr Aff. ¶¶ 2-4; Ex. to Springfield Defs.' Mot. Partial Summ. J.

Christopher Lebaroff, a ninth grade student at Kiefer Alternative School, subsequently purchased that same laptop for \$40 at a bus station, suspecting that it was stolen. Lebaroff Dep. at 9-10, 21, 28. Lebaroff later approached Plaintiff Susan Clements-Jeffrey, a long-term substitute teacher at Kiefer, and offered to sell her the laptop for \$60. Clements-Jeffrey Dep. at 72, 74. He told her that he no longer needed it because his aunt and uncle had given him a new laptop. *Id.* at 72. He also told her that his parents had given him permission to sell it. *Id.* at 82-

---

<sup>1</sup> Also pending is Plaintiffs' Motion in Limine to Exclude Testimony of Dr. Arthur J. Jipson (Doc. #93), Defendants' expert witness. That motion is the subject of a separate decision.

<sup>2</sup> As required when deciding a motion for summary judgment, the facts are construed in a light most favorable to the non-moving party. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986).

83. Lebaroff informed her that the laptop was currently “messed up” and inoperable, but that Albert Apple, another Kiefer teacher, was trying to fix it. *Id.* at 74-75. Clements-Jeffrey agreed to buy the laptop if Apple could repair it. *Id.* at 81.

Apple testified that Lebaroff told him that he had accidentally wiped the hard drive clean and could not reinstall the operating system because his aunt, who lived out of state, had the necessary discs. Apple Dep. at 25-28. Apple was able to reinstall the operating system using his own discs. He also reinstalled other software that was freely available. *Id.* at 44-45. After Apple repaired the computer, Lebaroff tried to rescind his offer to sell it, but Clements-Jeffrey insisted that he follow through with the deal. Clements-Jeffrey Dep. at 102-104. In June of 2008, Clements-Jeffrey paid Lebaroff for the laptop and took it home. *Id.* at 85.

Clements-Jeffrey, 52, was a widow. She had recently renewed a high school romance with Plaintiff Carlton “Butch” Smith, who lived in Boston. Because of the geographical distance separating them, they maintained their relationship largely through phone calls and the Internet. Smith Dep. at 15-17. They often exchanged sexually explicit images via webcams attached to their computers. They also exchanged sexually explicit email messages and instant messages. *Id.* at 19, 24. Plaintiffs believed that these communications were secure and private because their computers were password-protected. *Id.* at 85-87.

Unfortunately for Plaintiffs, this belief was unfounded. When the school

district purchased the laptops, it also entered into a contract with Absolute Software, Inc., a theft recovery service. After Powell filed his police report, Jason Graver, an information technology employee for the school district, contacted Absolute. Graver provided Absolute with a copy of the police report and, on April 21, 2008, authorized Absolute to proceed with gathering information to try to identify the user of the stolen laptop. Graver Dep. at 9, 14.

According to Timothy Smail, Absolute's manager of forensic and investigative services, the laptops were equipped with "LoJack for Laptops," a combination of hardware and software, that enabled Absolute to track stolen laptops. Smail Dep. at 16-22. Once Graver gave permission, Absolute activated a "silent alarm," in essence telling the laptop that it had been stolen. The stolen laptop was directed to report its IP address to Absolute the next time the laptop was connected to the Internet. *Id.* at 37-38. Once the IP address was identified, Absolute would generally assist in obtaining a warrant subpoena, directing the Internet service provider to provide identifying information about the computer user. *Id.* at 85; Magnus Dep. at 74-75, 139.

Absolute also caused the stolen laptop to download certain software, allowing theft recovery officers to gain remote access and to intercept email and other electronic communications sent to and from the stolen laptop. These interceptions would occur in "real time" without the user's knowledge. The officers could also capture screen shots of images from the computer's monitor.

Smail Dep. at 41-43, 61-62, 67-68, 73-74. The software also recorded all keystrokes and stored them on Absolute's server until the next time the computer was connected to the Internet, at which point the information could be retrieved by a theft recovery officer. *Id.* at 55-56, 59-60.

Once Clements-Jeffrey used the stolen laptop to connect to the Internet on June 8, 2008, LoJack was able to capture her IP address and transmit it to Absolute. At this point, the file was assigned to Kyle Magnus, one of Absolute's theft recovery officers. Magnus Dep. at 56-58. On June 21 and 22, 2008, Magnus captured keystrokes from the laptop and monitored Clements-Jeffrey's visits to various websites. *Id.* at 81-82. On June 24, 2008, over a 30-second period, while monitoring webcam communications between Clements-Jeffrey and Smith in "real time," Magnus took three screen shots of images appearing on the monitor. *Id.* at 106-110. In those screen shots, Clements-Jeffrey is not wearing any clothes and Smith is naked from the waist up. In one shot, Clements-Jeffrey has her legs spread apart. *Id.* at 112; Clements-Jeffrey Dep. at 171.

That same day, Magnus contacted Springfield police detective Geoffrey Ashworth to provide contact information for Susan Clements-Jeffrey, the person who he believed possessed the stolen laptop. Magnus Dep. at 119-20; Ashworth Dep. at 67. Magnus also sent Ashworth an introductory letter describing Absolute's business, Clements-Jeffrey's call log, and a warrant subpoena form. Ashworth Dep. at 65. In addition, Magnus sent copies of the communications that

he had captured from the stolen laptop, along with the three sexually explicit screen shots. *Id.* at 69-72.

Ashworth then downloaded Clements-Jeffrey's driver's license information, including her address and her picture, and compared it to the information he had received from Magnus. *Id.* at 68-69. On June 25, 2008, Ashworth and Springfield Police Lieutenant Noel Lopez went to Clements-Jeffrey's apartment to question her about the laptop. *Id.* at 89. According to Clements-Jeffrey, they knocked on her door. She was on the phone with Smith and ignored them until she heard them say "this is the police," and "we can get a warrant." She stepped out onto her landing. They asked her if her name was Susan and whether she had a laptop in her apartment. When she answered affirmatively, they demanded to see her laptop computer. At that point, one of the officers allegedly held up some papers and told her that they had a warrant. Clements-Jeffrey Dep. at 113-20, 123.

She went back inside. The officers followed her and looked around her apartment. At their request, she brought her laptop from the bedroom to the kitchen. *Id.* at 127-35. The officers noticed that the serial number had been torn off. They asked her how she had acquired the laptop. She explained that she had purchased it from Lebaroff. She denied having any idea that it was stolen. *Id.* at 141-43. They allegedly told her that she was stupid, and that she was under arrest. *Id.* at 144-45. Ashworth and Lopez told her that the laptop had been

stolen, and explained how they were able to trace the laptop to her using the LoJack software. *Id.* at 150. Ashworth then showed her the sexually explicit screen shots that Magnus had intercepted and sent to him. *Id.* at 147, 150, 171. Clements-Jeffrey claims that Ashworth laughed at her, called her stupid, and told her that she should have known better than to do that kind of stuff on the webcam. *Id.* at 152.

Ashworth and Lopez arrested Clements-Jeffrey for receiving stolen property. They handcuffed her and took her to the police station. *Id.* at 154. Ashworth allegedly continued to berate her about her use of the webcam, and again showed her the pictures and instant messages she had exchanged with Smith, calling them "disgusting." *Id.* at 170-72. Although she was charged and arraigned in the Clark County Municipal Court, the charge against her was dismissed on July 7, 2008.

Clements-Jeffrey and Smith filed suit in March of 2009, asserting numerous federal and state law claims. The Third Amended Complaint, filed on July 28, 2010, lists five defendants: the City of Springfield, Ashworth, Lopez, Absolute, and Magnus. Clements-Jeffrey seeks relief under 42 U.S.C. § 1983 against Ashworth and Lopez for alleged violations of her Fourth and Fourteenth Amendment rights. Plaintiffs also allege that Defendants violated the Electronic Communications Privacy Act and the Stored Communications Act. Finally, Plaintiffs bring a common law claim of invasion of privacy against Ashworth, Lopez, Magnus, and Absolute.

The Springfield Defendants concede that genuine disputes of material fact preclude summary judgment on that portion of Clements-Jeffrey's § 1983 claim related to the search of her apartment. However, they have moved for summary judgment on all of the other claims brought against them. The Absolute Defendants have moved for summary judgment on all claims brought against them.

## **II. Summary Judgment Standard**

Summary judgment must be entered "against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). The moving party always bears the initial responsibility of informing the district court of the basis for its motion, and identifying those portions of "the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any," which it believes demonstrate the absence of a genuine issue of material fact. *Id.* at 323; *see also Boretti v. Wiscomb*, 930 F.2d 1150, 1156 (6th Cir. 1991).

"Once the moving party has met its initial burden, the nonmoving party must present evidence that creates a genuine issue of material fact making it necessary to resolve the difference at trial." *Talley v. Bravo Pitino Rest., Ltd.*, 61 F.3d 1241, 1245 (6th Cir. 1995); *see also Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 250 (1986). Once the burden of production has so shifted, the party opposing summary judgment cannot rest on its pleadings or merely reassert its previous allegations, it



is not sufficient to “simply show that there is some metaphysical doubt as to the material facts.” *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586 (1986). Rule 56(e) “requires the nonmoving party to go beyond the [unverified] pleadings” and present some type of evidentiary material in support of its position. *Celotex*, 477 U.S. at 324. “The plaintiff must present more than a scintilla of evidence in support of his position; the evidence must be such that a jury could reasonably find for the plaintiff.” *Mich. Prot. & Advocacy Serv., Inc. v. Babin*, 18 F.3d 337, 341 (6th Cir. 1994).

Summary judgment “shall be rendered forthwith if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(c).<sup>3</sup> Summary judgment shall be denied “[i]f there are . . . ‘genuine factual issues that properly can be resolved only by a finder of fact because they may reasonably be resolved in favor of either party.’” *Hancock v. Dodson*, 958 F.2d 1367, 1374 (6th Cir. 1992) (citation omitted). In determining whether a genuine issue of material fact exists, a court must assume as true the evidence of the nonmoving party and draw all reasonable inferences in favor of that party. *Anderson*, 477 U.S. at 255. If the parties present conflicting evidence, a court may not decide which evidence

---

<sup>3</sup> Amendments to Federal Rule of Civil Procedure 56 became effective on December 1, 2010. Nevertheless, because Defendants’ motions were filed prior to that date, the prior version of the Rule is quoted here.

to believe, by determining which parties' affiants are more credible; rather, credibility determinations must be left to the fact-finder. 10A Wright, Miller & Kane, *Federal Practice and Procedure* Civil 3d § 2726 (1998).

In ruling on a motion for summary judgment (in other words, in determining whether there is a genuine issue of material fact), "[a] district court is not . . . obligated to wade through and search the entire record for some specific facts that might support the nonmoving party's claim." *InterRoyal Corp. v. Sponseller*, 889 F.2d 108, 111 (6th Cir. 1989), *cert. denied*, 494 U.S. 1091 (1990); *see also* *L.S. Heath & Son, Inc. v. AT&T Info. Sys., Inc.*, 9 F.3d 561 (7th Cir. 1993); *Skotak v. Tenneco Resins, Inc.*, 953 F.2d 909, 915 n.7 (5th Cir. 1992), *cert. denied*, 506 U.S. 832 (1992) ("Rule 56 does not impose upon the district court a duty to sift through the record in search of evidence to support a party's opposition to summary judgment . . . ."). Thus, a court is entitled to rely, in determining whether a genuine issue of material fact exists on a particular issue, only upon those portions of the verified pleadings, depositions, answers to interrogatories and admissions on file, together with any affidavits submitted, specifically called to its attention by the parties.

### **III. Analysis**

As noted above, Plaintiffs' claims include: (1) a 42 U.S.C. § 1983 claim based on alleged violations of Clements-Jeffrey's Fourth Amendment rights; (2) alleged violations of the Electronic Communications Privacy Act ("ECPA") and the

Stored Communications Act ("SCA"); and (3) a common law claim of invasion of privacy.

**A. Legitimate Expectation of Privacy**

Before turning to arguments specific to each of these causes of action, the Court will address the question of whether Plaintiffs had a legitimate expectation of privacy in their communications via the stolen laptop. In their Motion for Summary Judgment, the Absolute Defendants argue that, absent a legitimate expectation of privacy, each of Plaintiffs' claims fails as a matter of law.<sup>4</sup> See *Rakas v. Illinois*, 439 U.S. 128, 143 (1978) (holding that the ability to claim the protection of the Fourth Amendment depends upon whether the person has a legitimate expectation of privacy in the invaded place); *United States v. Mendoza*, 574 F.2d 1373, 1377 (5th Cir. 1978) (holding that defendants lacked standing under the ECPA to challenge the admissibility of a tape of an intercepted telephone conversation because "neither has a legitimate expectation of privacy"); *Sowards v. Norbar, Inc.*, 78 Ohio App.3d 545, 555, 605 N.E.2d 468, 474 (Ohio Ct. App. 1992) ("The tort of invasion of privacy vindicates an individual's reasonable expectation of privacy and seclusion.").

A determination of whether someone has a legitimate expectation of privacy depends on two factors: (1) "whether the individual, by conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that he sought to

---

<sup>4</sup> The Springfield Defendants later joined in this argument. Doc. #90, at 3.

preserve something as private;" and (2) "whether the individual's expectation of privacy is one that society is prepared to recognize as reasonable." *United States v. King*, 227 F.3d 732, 743-44 (6th Cir. 2000). The first factor is subjective and involves a question of fact; the second factor is objective and involves a question of law. *See United States v. Welliver*, 976 F.2d 1148, 1151 (8th Cir. 1992).

#### **1. Actual expectation of privacy**

With respect to the first factor, there is no genuine issue of material fact concerning whether Plaintiffs exhibited a subjective expectation of privacy in the laptop computer. Plaintiffs testified that they believed that their communications were secure because their computers were password-protected. Clements-Jeffrey Dep. at 255-56; Smith Dep. at 85-87. The use of such passwords indicates that Plaintiffs sought to keep their communications private. *See United States v. Lucas*, –F.3d–, 2011 WL 1775685, at \*8 (6th Cir. May 11, 2011) (noting that password protection may be considered in determining whether a privacy interest exists); *United States v. Aaron*, 33 F. App'x 180, 184 (6th Cir. 2002) (whether an individual manifested an intention to restrict third party access is a factor in determining whether a privacy interest exists).

Moreover, the intimate nature of Plaintiffs' instant messages and their webcam activities clearly supports a finding that they subjectively believed that their communications were entirely private. While at the police station, Clements-Jeffrey told Ashworth, "I am in the privacy of my own home. I am a grown

woman. I should be able to do what I want in the privacy of my own home.” *Id.* at 170. The Court further notes that Defendants do not seriously question that Plaintiffs had a subjective expectation of privacy.

## **2. Objectively reasonable expectation of privacy**

The parties, however, vehemently disagree about whether Plaintiffs’ subjective expectation of privacy was objectively reasonable. Although this is a question of law to be determined by the Court, *see Welliver*, 976 F.2d at 1151, in this particular case, its resolution turns on a question of fact –whether Plaintiffs knew or should have known that the laptop was stolen.

As the Tenth Circuit Court of Appeals has explained, “[b]ecause expectations of privacy derive in part from the right to exclude others from the property in question, lawful possession is an important consideration in determining whether a defendant had a legitimate expectation in the area searched.” *United States v. Lyons*, 992 F.2d 1029, 1031 (10th Cir. 1993).

An individual who *knowingly* possesses stolen property does not have a legitimate expectation of privacy in it. *See United States v. Tropiano*, 50 F.3d 157, 161 (2d Cir. 1995) (“we think it obvious that a defendant who knowingly possesses a stolen car has no legitimate expectation of privacy in the car”); *United States v. Hensel*, 672 F.2d 578, 579 (6th Cir. 1982) (holding that defendant who knowingly possessed a stolen truck had no legitimate expectation of privacy and therefore lacked standing to challenge its search). In a similar vein, the Ninth

Circuit has held that one who obtains a laptop by fraudulent means lacks a reasonable expectation of privacy in the contents of the hard drive. *See United States v. Caymen*, 404 F.3d 1196, 1201 (9th Cir. 2005).

Defendants argue that because Plaintiffs knew or should have known that the laptop computer being used by Clements-Jeffrey was stolen, Plaintiffs had no objectively reasonable expectation of privacy in their Internet communications.<sup>5</sup> Plaintiffs, however, deny that they knew or should have known that the laptop was stolen. This creates a question of fact that must be resolved by a jury.

Defendants maintain that there were several “red flags” that should have alerted Clements-Jeffrey to the fact that the laptop was stolen: (1) Lebaroff had a criminal history; (2) Lebaroff wanted only \$60 for the laptop; (3) the laptop’s hard drive had been “wiped” clean; and (4) the serial number on the bottom of the laptop had been scraped off (Ex. J to Meyer Decl.). In addition, Lebaroff testified that he “kind of suspected [Clements-Jeffrey] thought it was stolen.” Lebaroff Dep. at 36.

Clements-Jeffrey, however, testified that she did not know that Lebaroff had a criminal history. Clements-Jeffrey Dep. at 76. Although she knew that he was

---

<sup>5</sup> In their briefs, Defendants do not raise the question of whether, in a broader sense, individuals have any objectively reasonable expectation of privacy in communications over the Internet. Therefore, the Court need not decide this issue in the context of the pending motions for summary judgment. The issue is, however, raised in the report of Defendants’ expert witness, Dr. Arthur J. Jipson, and was addressed in the context of the decision ruling on Plaintiffs’ motion in limine to exclude his testimony.

involved in Project Jericho, a program for individuals who had “issues with tagging” (defacing property by spray-painting it), she was unaware that he had been ordered to participate in that program by the juvenile court system. *Id.* at 77-79. She testified that she did not suspect that he was offering to sell stolen property. *Id.* at 76. The computer looked like the same laptop he had been bringing to class, and she believed him when he told her that his aunt and uncle had just given him a new one, and that he had his parents’ permission to sell the old one. *Id.* at 72-73, 82-83.

Moreover, she knew nothing about the price of laptops. She did not consider Lebaroff’s \$60 offer “too good to be true,” particularly in light of the fact that he disclosed to her that, at that time, the computer was not working at all, and it was already two years old. *Id.* at 76, 91, 94, 143. Because she knew very little about computers, she attached no significance to the fact that the operating system was not working. In addition, she testified that she did not notice that the serial number had been scraped off the laptop. *Id.* at 97. Albert Apple also testified that he noticed nothing unusual about the serial number on the laptop. Apple Dep. at 22-23.

Clements-Jeffrey testified that she never suspected that the laptop was stolen. Clements-Jeffrey Dep. at 106. Her conduct when the police appeared at her house to question her about the laptop is consistent with this testimony. When asked if she knew the laptop was stolen, she replied, “[o]f course not,” and told

the police that there must be some misunderstanding. *Id.* at 143-44. Magnus testified he was on the phone with Ashworth during the officers' questioning of Clements-Jeffrey. When Ashworth told her that she was being charged with receiving stolen property, "she screamed 'what,' in all caps question marks exclamation point.'" Magnus Dep. at 121.

Based on the evidence presented, a reasonable jury could find that Clements-Jeffrey neither knew nor should have known that the laptop computer she bought from Lebaroff was stolen. Summary judgment on this issue is therefore inappropriate. The Court now turns to the arguments specific to each of Plaintiffs' claims.

#### **B. Unreasonable Search and Seizure**

Count I of the Third Amended Complaint alleges as follows:

By participating in a grossly excessive search and seizure of sexually explicit images depicting Plaintiffs when Defendants Ashworth and Lopez were tracing the theft of a laptop computer from its original owner and, beyond any need in number or content, used hard copies of those images in arresting and holding Plaintiff Clements-Jeffrey, Defendants Ashworth and Lopez violated Plaintiffs' Fourth and Fourteenth Amendment rights, and the search of her apartment without a warrant when her consent was duplicitously secured.

Third Amd. Compl. ¶ 62.

Clements-Jeffrey seeks damages under 42 U.S.C. § 1983, which provides an avenue of recovery against state actors who subject individuals to the deprivation of federal rights. This statute "'is not itself a source of substantive rights,' but merely provides 'a method for vindicating federal rights elsewhere



conferred.'" *Graham v. Connor*, 490 U.S. 386, 393-94 (1989) (quoting *Baker v. McCollan*, 443 U.S. 137, 144 n. 3 (1979)). In order to recover under § 1983, a plaintiff must prove that the defendant, while acting under color of state law, violated rights secured by the Constitution or laws of the United States. See *Adickes v. S.H. Kress & Co.*, 398 U.S. 144, 150 (1970).

It appears to be undisputed that Ashworth and Lopez were acting under color of state law during the events in question. The only question is whether they engaged in an unreasonable search and seizure in violation of the Fourth Amendment to the United States Constitution.<sup>6</sup>

Ashworth and Lopez concede that genuine issues of material fact exist concerning the warrantless entry into Clements-Jeffrey's apartment. Therefore, they have not moved for summary judgment on that portion of her § 1983 claim. In their Motion for Partial Summary Judgment, they argue that they had probable cause to believe that the laptop was stolen and was subject to a lawful seizure. They also argue that they are entitled to qualified immunity.

---

<sup>6</sup> After considerable briefing, it appears that the parties now agree that Plaintiffs have cited to the Fourteenth Amendment not because they are alleging a separate due process claim, but rather because the Fourth Amendment is made applicable to the states via the Fourteenth Amendment. See *New Jersey v. T.L.O.*, 469 U.S. 325, 334 (1985).

In her response brief, Clements-Jeffrey clarifies the focus of her § 1983 claim. She concedes that the officers had probable cause to seize her computer. She maintains, however, that Ashworth and Lopez violated her constitutional rights by using the sexually explicit communications, previously intercepted by Absolute and Magnus, to arrest her, to berate her, and to humiliate her. Clements-Jeffrey maintains that the scope of that search and seizure was unreasonable because, once Absolute had her IP address, nothing more was needed. Absolute could have given her IP address to the Springfield Police Department, which, in turn, could have obtained contact information for her through her Internet service provider. Clements-Jeffrey argues that there was no need for Absolute to intercept her private communications or pass them on to the police, and there was no need for Ashworth and Lopez to confront her with those sexually explicit communications during the course of her arrest.

Even though the Court has found that genuine issues of material fact exist concerning whether Plaintiffs had a legitimate expectation of privacy, this does not foreclose summary judgment in favor of Ashworth and Lopez on this particular portion of Clements-Jeffrey's § 1983 claim.

The officers argue that they are entitled to qualified immunity. The Court agrees. "Qualified immunity is an affirmative defense that shields government officials 'from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person

would have known.’” Estate of Carter v. City of Detroit, 408 F.3d 305, 310 (6th Cir. 2005) (quoting Harlow v. Fitzgerald, 457 U.S. 800, 818, (1982)).

As the Supreme Court explained in Saucier v. Katz, 533 U.S. 194 (2001), a claim of qualified immunity involves a two-step inquiry. First, the court must determine whether the facts, viewed in the light most favorable to the plaintiff, show that a statutory or constitutional violation has occurred. Id. at 201. Second, the court must determine whether the right at issue was clearly established. The relevant inquiry is “whether it would be clear to a reasonable officer that his conduct was unlawful in the situation he confronted.” Id. at 202. If the answer to either question is “no,” the officer is entitled to qualified immunity. Id. at 201-202<sup>7</sup>

In this case, viewing the facts in the light most favorable to the plaintiffs, the Court finds no Fourth Amendment violation with respect to this portion of Plaintiffs’ claim. Even if Clements-Jeffrey had a legitimate expectation of privacy, there is simply no legal basis for holding Ashworth and Lopez liable under § 1983 for their “use” of the sexually explicit communications allegedly illegally intercepted by Absolute and Magnus.

Clements-Jeffrey concedes that, as a general rule, the Fourth Amendment does not apply to searches and seizures by private actors. *See Burdeau v.*

---

<sup>7</sup> In *Pearson v. Callahan*, 555 U.S. 223 (2009), the Supreme Court held that these two factors need not be considered in any particular order.

*McDowell*, 256 U.S. 465, 475 (1921). She also concedes that when a private party presents evidence to the police, it is “not incumbent on the police to stop her or avert their eyes.” *Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971). See also *Walter v. United States*, 447 U.S. 649, 656 (1980) (holding that a wrongful search or seizure by a private party “does not deprive the government of the right to use evidence that it has acquired lawfully”).

In *United States v. Lambert*, 771 F.2d 83 (6th Cir. 1985), the court held that “the Fourth Amendment proscribes only governmental action and does not apply to a search or seizure, even an unreasonable one, conducted by a private individual *not acting as an agent of the government or with the participation or knowledge of any governmental official.*” *Id.* at 89 (emphasis added). Clements-Jeffrey argues that Absolute and Magnus were acting as “agents” of the Government when the search and seizure took place. She maintains that they illegally intercepted her private communications, and exceeded the scope of a reasonable search and seizure by continuing to monitor her activities even after having enough information to identify her as the user of the stolen laptop. Magnus then turned those sexually explicit communications over to Ashworth and Lopez. Clements-Jeffrey argues that because Ashworth and Lopez acted “in tandem” with Magnus, using the information provided to arrest her for receipt of stolen property, they should be held liable for the unreasonable search and seizure.

The Court rejects this argument. In determining whether a private party is acting as a government agent, two facts must be proven: "First, the police must have must have instigated, encouraged, or participated in the search. . . Second, the individual must have engaged in the search with the intent of assisting the police in their investigative efforts." *Lambert*, 771 F.2d at 89.

In this case, there is absolutely no evidence that the police knew anything at all about Absolute's attempts to identify the user of the stolen laptop until June 23, 2008, when Magnus provided Ashworth with contact information for Clements-Jeffrey, along with copies of all of the intercepted communications. Plaintiffs have presented no evidence that the Government instigated, encouraged, or participated in Absolute's search. Therefore, the first element clearly cuts against a finding that the Absolute Defendants were acting as agents of the Government, *i.e.*, the Springfield police officers.

As to the second element, Clements-Jeffrey maintains that "Absolute's *raison d'être* is law enforcement." Doc. #82, at 27. It exists in order to help the police recover laptop computers that have been stolen from Absolute's clients. Absolute supplied all of the information that Ashworth and Lopez needed to arrest Clements-Jeffrey for receipt of stolen property. Absolute denies that it is in the business of law enforcement; it maintains that it exists to help its customers recover their stolen computers.

Regardless of whether Absolute engaged in the search with the intent of passing along information to the police, Clements-Jeffrey cannot prove that the police instigated, encouraged or participated in the search. Therefore, the Absolute Defendants cannot be deemed agents of the Government.

Moreover, even if the Court concluded that the Absolute Defendants were acting as agents of the Government, this would not provide any basis for imposing personal liability on Ashworth or Lopez under § 1983.<sup>8</sup> Their allegedly illegal conduct cannot be imputed to Ashworth and Lopez for purposes of § 1983 liability. Rather, the Court may look only to alleged conduct of the officers. *See Ruiz v. McDonnell*, 299 F.3d 1173, 1182 (10th Cir. 2002) (“Generally, state actors may only be held liable under § 1983 for their own acts. . . .”). With respect to Ashcroft and Lopez, Clements-Jeffrey alleges that they used the unlawfully intercepted communications to arrest her and to berate and humiliate her. These allegations do not constitute an unreasonable search or seizure under the Fourth Amendment.

In *United States v. King*, 55 F.3d 1193 (6th Cir. 1995), the Sixth Circuit

---

<sup>8</sup> In a criminal case, the existence of an agency relationship could result in the suppression of evidence. *See Lambert*, 771 F.2d at 89; *United States v. Jarrett*, 338 F.3d 339, 344 (4th Cir. 2003). Similarly, in a civil case, the existence of an agency relationship could transform a private party into a “state actor” for purposes of imposing personal liability under § 1983. *See Chapman v. Higbee Co.*, 319 F.3d 825, 833 (6th Cir. 2003) (explaining the circumstances under which a private party may be deemed a “state actor” under § 1983). Neither of these situations is applicable in this case. Clements-Jeffrey has not sued the Absolute Defendants under § 1983.

held that “[o]nce a private search is conducted, the government’s subsequent use of the information obtained in the private search does not implicate the Fourth Amendment as long as the government’s use does not exceed the scope of the private search.” *Id.* at 1196 (citing *United States v. Jacobsen*, 466 U.S. 109, 116-17 (1984)). In this case, there is absolutely no evidence that Ashworth and Lopez expanded the scope of the search and seizure conducted by the Absolute Defendants. They did not make any effort to intercept any other communications, and did not ask Magnus to conduct any further surveillance. They simply took all of the information given to them and used it to arrest Clements-Jeffrey for receipt of stolen property. Using this information in this manner does not constitute an unreasonable search or seizure.

Clements-Jeffrey also alleges that Ashworth and Lopez violated her Fourth Amendment rights by using the sexually explicit communications to humiliate her and berate her during the course of the arrest. Defendants deny that they acted inappropriately, but even if they did behave in an unprofessional manner, such conduct does not implicate the Fourth Amendment. *See United States v. Oliver*, 363 F.3d 1061, 1067 (10th Cir. 2004) (noting that “protection against rude, officious, or intrusive police questioning is not a core concern of [the Fourth Amendment]”); *Martin v. Ross*, No. 1:08-cv-199, 2008 WL 5070440, at \*3 (N.D. Ind. 2008) (“The Fourth Amendment, however, does not protect citizens from being generally harassed and treated unfairly or unprofessionally by a police

department or individual police officers; it protects citizens against unreasonable searches and seizures.”)

Because the officers’ conduct did not violate the Fourth Amendment, they are entitled to qualified immunity, and summary judgment is therefore appropriate on this portion of the § 1983 claim. The Court notes that Clements-Jeffrey’s Fourth Amendment claim stemming from the officers’ warrantless search of her apartment remains pending.

**C. Electronic Communications Privacy Act and Stored Communications Act**

In Count II of the Third Amended Complaint, Plaintiffs allege that:

By intercepting, downloading, making hard copies, using, and retaining sexually explicit images depicting Plaintiffs when Defendants were tracing the theft of a laptop computer from its original owner and lacked any need in number or content for those images, Defendants violated the Electronic Communications Privacy Act [“ECPA”] and the Stored Communications Act [“SCA”].

Third Amd. Compl. ¶ 64.

**1. Relevant Law**

Title I of the Electronic Communications Privacy Act (“ECPA”) protects against the unauthorized interception of wire, oral, or electronic communications. With certain exceptions enumerated in the statute, it establishes civil and criminal liability for any person who:

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;



\* \* \*

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection[.]

18 U.S.C. § 2511(1).

Title II of the ECPA, also known as the Stored Communications Act ("SCA"), prohibits intentional unauthorized access of stored electronic communications and transactional records. Again, with certain enumerated exceptions, the SCA establishes civil and criminal liability for whoever:

- (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
- (2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.

18 U.S.C. § 2701.

The Court turns first to the claims arising under Title I of the ECPA.

## **2. ECPA Claims**

### **a. Defenses Raised by Absolute Defendants**

Plaintiffs maintain that the Absolute Defendants violated the ECPA by intentionally intercepting electronic communications in violation of 18 U.S.C. §

2511(a), and by intentionally disclosing them to the Springfield police officers in violation of 18 U.S.C. § 2511(c).

The Absolute Defendants argue that they are entitled to summary judgment on these claims for several reasons. They again argue that because Plaintiffs had no reasonable expectation of privacy, they do not state a claim under the ECPA. As previously held, however, genuine issues of material fact preclude summary judgment on this issue.

**i. Computer Trespasser**

The Absolute Defendants argue that Plaintiffs were “computer trespassers,” defined in 18 U.S.C. § 2510(21)(A) as “a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer.” The term “computer trespasser” is used in 18 U.S.C. § 2511(i), which states as follows:

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's

communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

18 U.S.C. § 2511(i).

As Plaintiffs correctly point out, § 2511(i) is completely inapposite because the Absolute Defendants, who intercepted Plaintiffs' electronic communications, were not "acting under color of law."<sup>9</sup> Therefore, this defense provides no basis for awarding summary judgment in favor of the Absolute Defendants.

## **ii. Good Faith Defense**

The Absolute Defendants also argue that the "good faith defense" set forth in 18 U.S.C. § 2520(d) applies. That subsection provides that:

A good faith reliance on –

- (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;
- (2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or
- (3) a good faith determination that section 2511(3) or 2511(2)(i) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

18 U.S.C. § 2520(d).

---

<sup>9</sup> The Absolute Defendants maintain that because they were working on behalf of their customer, a public school district, they should be deemed to be acting "under color of law." This argument is wholly without merit.

The Absolute Defendants argue that §2520(d)(3) provides them with a safe harbor. That subsection refers to § 2511(3), which sets forth certain circumstances under which “a person or entity providing an electronic communication service to the public” may divulge the contents of certain communications. In turn, an “electronic communication service” is defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). An obvious example would be an Internet service provider. Because the Absolute Defendants do not provide an “electronic communication service to the public,” this exception does not apply. Subsection 2520(d)(3) also refers to § 2511(2)(i), which, as discussed above, is inapplicable because the Absolute Defendants were not “acting under color of law.” For these reasons, the Court finds that the “good faith” defense set forth in 18 U.S.C. § 2520(d)(3) is inapplicable and provides no basis for awarding summary judgment in favor of the Absolute Defendants.

### **iii. Public Policy**

Finally, the Absolute Defendants argue that, as a matter of public policy, the rights of a user of stolen property can never trump the rights of the legal owner of the stolen property. They maintain that the legal owner of the stolen laptop should be able to take steps to locate and recover that property.

In support, they cite to *United States v. Caymen*, 404 F.3d 1196 (9th Cir. 2005). In that case, the defendant used a stolen credit card to purchase a

computer from a business supply store. When the credit card's owner complained, the police obtained a search warrant. During a search of the defendant's home, they discovered the laptop at issue. The police contacted the store to get permission to look at the computer before returning it to the store. The store's owner granted permission and specifically requested that the police search the hard drive to make sure that it did not have anything "that shouldn't be there." *Id.* at 1198. The police found child pornography. The defendant was charged with possession of child pornography and fraudulent use of a credit device.

He moved to suppress the evidence of the pornography found on the laptop, arguing that the store had no right to consent to the search because the computer belonged to him. The court held that he had no standing to challenge the legality of the search because he had no reasonable expectation of privacy, having purchased the computer with a stolen credit card. *Id.* at 1201.

The court noted that "[w]hatever possessory interest a thief may have, that interest is subordinate to the rights of the owner." *Id.* at 1200-01. The court equated the defendant's fraudulent conduct to that of a thief, and found that he was not entitled to prevent the store from granting permission to search the computer. *Id.* at 1201.

*Caymen* is, of course, factually distinguishable, in that the defendant in that case was clearly culpable. In contrast, if Clements-Jeffrey is to be believed, she was an innocent purchaser who had no idea that the laptop was stolen.

Defendants have cited to no cases in which an innocent purchaser of stolen property was found not to have a reasonable expectation of privacy, and no cases in which that person's privacy interests were found to be subordinate to the rights of the person claiming to be the rightful owner of the stolen property.

In support of their motion for summary judgment, the Absolute Defendants also cite to the case of *State v. Oliveras*, –So.3d –, 2011 WL 2923696 (Fla. Dist. Ct. App. July 22, 2011). In that case, defendant was charged with stealing two computers from someone's luggage. One of those computers was equipped with Absolute's theft recovery software. Absolute was able to trace the location of the computer and, at the victim's request, provided that information to the police. The police obtained a search warrant and recovered the stolen computers from defendant's residence.

The defendant moved to suppress the evidence, citing the officer's failure to comply with § 934.23(1), Florida Statutes. That statute provides, in part: "An investigative or law enforcement officer may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for 180 days or less only pursuant to a warrant issued by the judge of a court of competent jurisdiction." Defendant argued that the search warrant was deficient because the police had not obtained a court order or subpoena to retrieve the information from Absolute, as required by the statute. The district court

granted the motion to suppress, albeit on slightly different grounds.

The appellate court reversed. It found § 934.23(1) to be inapplicable, noting that the officer had not requested any information from Absolute. Rather, the victim requested Absolute to provide the information to the police. The court noted that § 934.22(2) permits an electronic communications provider to divulge the contents of a communication to an agent of an addressee or intended recipient of the communication. The court concluded as follows:

Here, the victim is the intended recipient of the tracking and identification information because she paid for that information to be captured from her own computer, pursuant to her contract with Absolute. The victim was entitled to the information and to request Absolute to provide it to Officer Hall. Moreover, the information gleaned by Absolute pertains only to the thief, who lacked any reasonable expectation of privacy with respect to any communication he transmitted to, through, or from the stolen computer.

*Oliveras*, 2011 WL 2923696, at \*4.<sup>10</sup>

In the Court's view, the holdings in *Oliveras*, which are based on Florida state law, are unremarkable and do little to support Defendant's position. There is no question that a thief lacks a reasonable expectation of privacy in a stolen laptop. However, it is undisputed that Clements-Jeffrey is not a thief. The question of whether she had a reasonable expectation of privacy turns on the issue of whether she knew or should have known that the laptop she purchased was stolen.

---

<sup>10</sup> The court in *Oliveras* did not address the question of whether Absolute was an "electronic communications provider."

Moreover, in *Oliveras*, it appears that only “tracking and identification information” was turned over to the police. In contrast, in this case, Absolute provided the Springfield police not only with Clements-Jeffrey’s IP address, but also with screen shots of Plaintiffs’ webcam activity and keystrokes that Absolute had intercepted.

Notably, Plaintiffs do not argue that the school district could take no action to recover its stolen property. Plaintiffs argue, however, that any action taken must be within the confines of the law. That, in essence, is the heart of this case. Plaintiffs argue that, in attempting to recover the school district’s stolen property, Defendants violated their constitutional and statutory rights, and invaded their privacy.

The Absolute Defendants cite to several articles detailing the creative steps that owners of stolen laptops have taken to recover their property. Many laptop computers are equipped with remote access tools such as “GoToMyPC,” “Back to my Mac,” and “Mobile Me.” These remote access tools can sometimes double as theft recovery products. When a laptop is stolen, its rightful owner can log on to another computer, and cause his own computer to report its location to him. He can also cause his computer to take and send photographs of its user. See Exhs. to Jipson Expert Report. The Absolute Defendants contend “[t]hat is all that happened in this case.” Doc. #78, at 18. Acting on behalf of the rightful owner of the laptop, the Absolute Defendants used remote access tools to track down the



stolen computer.

The Absolute Defendants ignore one crucial distinction. It is one thing to cause a stolen computer to report its IP address or its geographical location in an effort to track it down. It is something entirely different to violate federal wiretapping laws by intercepting the electronic communications of the person using the stolen laptop.

The ECPA carves out no exception allowing a private entity to intentionally intercept electronic communications for the purpose of gathering information to facilitate recovery of a stolen laptop. As Plaintiffs contend, it would be inappropriate for the Court to legislate a “public policy” exception to the ECPA. *See Nix v. O’Malley*, 160 F.3d 343, 350 (6th Cir. 1998) (“Ohio and federal wiretap law explicitly permit disclosures in certain instances (pursuant to valid warrants, for example), but their plain language allows no further exceptions.”). Therefore, the Absolute Defendants are not entitled to summary judgment on this claim.

**b. Defenses Raised by Springfield Defendants**

Plaintiffs allege that Ashworth disclosed the illegally intercepted electronic communications to Lopez, and possibly to others in the police department, in violation of 18 U.S.C. § 2511(c). Plaintiffs also allege that the Springfield Defendants intentionally “used” those electronic communications in violation of 18

U.S.C. § 2511(d). The Springfield Defendants offer several defenses.<sup>11</sup>

**i. Unlawful Interception**

The Springfield Defendants note that unless Plaintiffs can prove an unlawful interception by the Absolute Defendants, the Springfield Defendants cannot be liable for unlawful disclosure or use of that information. *See Nix*, 160 F.3d at 348. As the Court has previously held, the Absolute Defendants are not entitled to summary judgment based on the asserted defenses to the ECPA. Neither, then, are the Springfield Defendants.

**ii. Reason to Know Interception Was Unlawful**

The Springfield Defendants next argue that because they neither knew nor had reason to know that the Absolute Defendants' interception of Plaintiffs' communications was unlawful, the Springfield Defendants cannot be held liable under the ECPA. *See Nix*, 160 F.3d at 348.

In *Nix*, the Sixth Circuit held that the plaintiff:

must show that the defendants knew "1) [that] the information used or disclosed came from an intercepted communication, and 2) sufficient facts concerning the circumstances of the interception such that the defendant[s] could, with presumed knowledge of the law, determine that the interception was prohibited in light of [the ECPA]."

---

<sup>11</sup> This is the only claim brought against the City of Springfield. The factual and legal basis for the claim against the City is ill-defined, and is not addressed in the parties' briefs. The Absolute Defendants' Motion for Summary Judgment states that "Plaintiffs recently dismissed defendant The City of Springfield, Ohio." Doc. #78, at 1 n.1. The Court notes, however, that there is not currently any docket entry to that effect.

*Id.* at 349-50 (quoting *Thompson v. Dulaney*, 970 F.2d 744, 749 (10th Cir.1992)).

In this case, it is undisputed that Ashworth and Lopez knew that the information given to them came from an intercepted communication. Magnus told them that he had taken screen shots of Plaintiffs' webcam activity and captured Clements-Jeffrey's keystrokes. Ashworth Dep. at 61.

The Springfield Defendants maintain, however, that they had no reason to doubt the legality of Absolute's conduct. Absolute was in the theft recovery business and did exactly what the school district had paid it to do. It activated the theft recovery software, gathered information about the user of the stolen laptop, and passed that information to the police so that the stolen property could be recovered.

Ashworth testified that he was not familiar with federal wiretapping laws, and he assumed that Absolute had the right to intercept Plaintiffs' electronic communications and pass the information along to him. Ashworth Dep. at 62-64. In *Nix*, the Sixth Circuit held that a defendant "cannot escape liability merely by claiming he did not believe the interception occurred illegally." *Id.* at 349. Defendants are presumed to have knowledge of the law. *Id.* at 349-50.

The ECPA contains no exception that would allow a private company to intercept electronic communications under the circumstances presented here. In the Court's view, there is enough evidence from which a reasonable jury could find that the Springfield Defendants should have known that it was illegal for the

Absolute Defendants to intercept Plaintiffs' private communications. Summary judgment on this basis is therefore unwarranted.

**iii. Clean Hands Exception**

The Springfield Defendants also argue that, even if they knew or should have known that the interception was unlawful, they are immune from liability pursuant to a "clean hands" exception to the ECPA. This exception was first recognized by the Sixth Circuit in *United States v. Murdock*, 63 F.3d 1391, 1404 (6th Cir. 1995). At issue was the applicability of 18 U.S.C. § 2515, the subsection of the ECPA that prohibits illegally intercepted wire or oral communications from being admitted as evidence in trials, hearings, or other adversarial proceedings. The Sixth Circuit created a "clean hands" exception to this statute, holding that this exclusionary rule did not apply to the government if the government played no part in the illegal interception.

The Springfield Defendants seek to extend this holding to civil suits, and urge the Court to find that so long as they did not play a part in the illegal interception of the communications, they cannot be held liable for their subsequent "disclosure" or "use" of that information.

The ECPA sets forth the following exceptions for law enforcement officers:

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making

or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

18 U.S.C. § 2517(1) and (2). These exceptions are most frequently applied in cases involving a judicially-approved wiretap.

The Springfield Defendants do not rely on these statutory defenses, perhaps because it is questionable whether the officers obtained knowledge of the contents of Plaintiffs' electronic communications "by any means authorized" by the ECPA. Nevertheless, this statute is at the heart of the decisions in several of the other cases cited by the parties.

In *Forsyth v. City of Dallas*, 19 F.3d 1527 (5th Cir. 1994), a civil suit alleging violations of the Federal Wiretap Act, the court applied a "clean hands" exception and found that police officers who used and disclosed information derived from an illegally intercepted communication were not liable for damages. The court held that § 2517(1) and (2) authorized police officers who did not participate in or procure the illegally intercepted communications to disclose and use those communications in conducting a preliminary internal affairs investigation. *Id.* at 1545.

*Forsyth* was cited with approval by the Sixth Circuit in *Doe v. S.E.C.*, 86 F.3d 589 (6th Cir. 1996). In *Doe*, a securities trader sued the Securities and

Exchange Commission ("SEC") seeking to enjoin its use of a tape recording made by a private party in violation of the ECPA. The district court issued the requested injunctions, but the Sixth Circuit vacated them. Relying on *Murdock* and *Forsyth*, the court held that because the SEC did not "encourage or participate in the wiretapping itself," and because it used the protected information in an appropriate manner, the SEC was permitted, under 18 U.S.C. § 2517(1) and (2), to use and disclose the contents of the tape recording in a preliminary investigation. *Doe*, 86 F.3d at 596. The court concluded that the civil action was "barred by the 'clean hands' defense." *Id.* at 598.

Despite the holding in *Doe*, the continued viability of the "clean hands" defense is questionable. As the Sixth Circuit noted in *Nix v. O'Malley*, 160 F.3d 343, 350-51 (6th Cir. 1998), Judge Merritt filed a "vigorous dissent" in the *Doe* case. More importantly, the *Doe* decision was later vacated. *See Doe v. S.E.C.*, 86 F.3d 599 (6th Cir. 1996). On rehearing en banc, the court again vacated the injunctions on other grounds, with no discussion of *Murdock*. *See Smith v. S.E.C.*, 129 F.3d 356 (6th Cir. 1997).

In *Nix*, however, the Sixth Circuit, citing the importance of privacy interests, cautioned against judicially-created exceptions to federal and state wiretapping laws prohibiting use and disclosure of illegally acquired information. *Nix*, 160 F.3d at 350-51. Moreover, in civil actions brought under the ECPA, many courts have criticized *Murdock* and have rejected the availability of a "clean hands" defense.

*See, e.g., Berry v. Funk*, 146 F.3d 1003, 1013 (D.C. Cir. 1998) (rejecting *Murdock* and *Forsyth* as contrary to the plain language of § 2517); *Chandler v. United States Army*, 125 F.3d 1296, 1302 (9th Cir. 1997) (“we cannot reconcile the Sixth Circuit reading [in *Murdock*] with the statutory language”); *Spetalieri v. Kavanaugh*, 36 F. Supp.2d 92, 117-18 (N.D.N.Y. 1998) (“a plain reading of § 2517 in conjunction with the purpose behind the legislation evinces that Congress did not intend to except illegally obtained information that is provided to law enforcement officers when those officers know the information to have been obtained in violation of the Wiretap Statute.”).

Because there is no authoritative Sixth Circuit case law extending the “clean hands” exception recognized in *Murdock* to cases seeking damages in a civil suit, and because *Murdock* has been soundly criticized both inside and outside the Sixth Circuit, the Court is not inclined to grant summary judgment to the Springfield Defendants on the basis of a “clean hands” defense. Nevertheless, because the law in this area is not clearly established, the Court finds that Ashworth and Lopez are entitled to qualified immunity on the ECPA claim.

#### **iv. Qualified Immunity**

As noted above, summary judgment based on qualified immunity is appropriate when it would not be clear to a reasonable officer that his conduct was unlawful in the situation he confronted. *Saucier*, 533 U.S. at 202. “In the context of qualified immunity, preexisting, clearly established law refers to binding

precedent from the Supreme Court, the Sixth Circuit, the district court itself, or other circuits that is directly on point.” *Kennedy v. City of Villa Hills*, 635 F.3d 210, 214 -215 (6th Cir. 2011) (internal quotation omitted).

In this case, there is no Supreme Court decision and no Sixth Circuit decision extending the “clean hands” exception recognized in *Murdock* to civil cases in which police officers are sued for disclosing or using communications illegally intercepted by a third party. Although *Doe* comes close to being on point, that decision was vacated. Moreover, there is no clear consensus among the other circuits concerning the availability of the “clean hands” defense. Compare *Forsyth*, 19 F.3d 1527 (5th Cir. 1994), with *Berry*, 146 F.3d 1003 (D.C. Cir. 1998), and *Chandler*, 125 F.3d 1296 (9th Cir. 1997). Because the law is not clearly established, Ashworth and Lopez are entitled to qualified immunity on the ECPA claims.

### **3. SCA Claim**

The factual and legal basis for Plaintiffs’ SCA claim is somewhat cloudy. As noted earlier, with certain exceptions, the SCA establishes civil liability for whoever:

- (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
- (2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.



18 U.S.C. § 2701. The SCA also prohibits disclosure of contents of stored electronic communications by “a person or entity providing an electronic communication service to the public,” 18 U.S.C. § 2702, and sets forth the circumstances under which a governmental entity can require disclosure of stored electronic communications by providers of an “electronic communication service” or a “remote computing service,” 18 U.S.C. § 2703.

In their Motion for Partial Summary Judgment, the Springfield Defendants argue that they cannot be held liable under the SCA because they did not “intentionally access” any stored data, *see* 18 U.S.C. § 2701, and they do not provide “electronic communication service” or “remote computing service” to the public, *see* 18 U.S.C. §§ 2702 and 2703. Plaintiffs fail to respond to this argument, impliedly conceding that they have no viable claim under the SCA against the Springfield Defendants. Finding no genuine issue of material fact, the Court sustains the Springfield Defendants’ motion for summary judgment on the SCA claim.

In their Motion for Summary Judgment, the Absolute Defendants argue that they cannot be liable under 18 U.S.C. § 2701 because they did not “intentionally access” any stored electronic communications “without authorization.” They note that the authorization form signed by Jason Graver stated that he was aware that by downloading the remote access tools, “Theft Recovery Officers may have the ability to view and recover any files that are present on the aforementioned

computer.” Graver Dep. at 14. The Absolute Defendants therefore maintain that they had authorization from the school district, the rightful owner of the stolen laptop, to access the stored electronic communications.

Plaintiffs do nothing to directly refute this argument. In a footnote in their Memorandum in Opposition to the Absolute Defendants’ Motion for Summary Judgment, Plaintiffs simply state that “Absolute’s keystroke capture apparently violated the SCA, though the focus of the analysis in this memorandum is on the ECPA.” Doc. #110, at 28 n.3. Plaintiffs argue that the stolen laptop was “arguably” a “facility” as that term is used in 18 U.S.C. § 2701 “because it was the conduit ‘through which’ the Internet services provider operated and stored the keystrokes Absolute then captured.” *Id.*

Plaintiffs note elsewhere in their brief, *id.* at 11-12, that Graver testified that although he knew that Absolute would attempt to discover the IP address of the user of the stolen laptop, he was not aware that Absolute would be intercepting Plaintiffs’ communications with third parties. Graver Dep. at 23, 73-74. Plaintiffs imply that because Graver did not knowingly consent to the keystroke capture at issue, any access of those stored electronic communications was unauthorized.

The Absolute Defendants’ reply brief is completely silent as to the SCA claim. In the Court’s view, they have failed to establish the absence of a genuine issue of material fact. Based on the evidence presented, a reasonable jury could find that, with respect to the keystroke capture, the Absolute Defendants

“intentionally accessed” data stored on the laptop “without authorization” to do so.

The Court therefore finds that the Absolute Defendants are not entitled to summary judgment on the SCA claim.

#### **D. Invasion of Privacy**

In Count III of the Third Amended Complaint, Plaintiffs allege that:

By intercepting, downloading, making hard copies, using, and retaining sexually explicit images depicting Plaintiffs when Defendants Ashworth, Lopez, Magnus, and Absolute were tracing the theft of a laptop computer from its original owner and lacked any need in number or content for those images, Defendants Ashworth, Lopez, Magnus, and Absolute have intentionally invaded Plaintiffs’ privacy.

Third Amd. Compl. ¶ 66.

##### **1. Relevant Law**

Ohio recognizes a cause of action for “wrongful intrusion into one’s private activities in such a way as to outrage or cause a person of ordinary sensibilities to suffer mental suffering, shame or humiliation.” *Housh v. Peth*, 165 Ohio St. 35, 133 N.E.2d 340 (Ohio 1956), ¶ 2 of syl. The Ohio Supreme Court has held that, “[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.” *Sustin v. Fee*, 69 Ohio St.2d 143, 145, 431 N.E.2d 992, 993-94 (Ohio 1982) (quoting Restatement of Torts 2d § 652B).

##### **2. Absolute Defendants**

In their Motion for Summary Judgment, the Absolute Defendants argue that

Plaintiffs' invasion of privacy claim fails because Plaintiffs had no reasonable expectation of privacy in their communications via the stolen laptop. As previously discussed, genuine issues of material fact preclude summary judgment on this issue.

The Absolute Defendants also note that their conduct was "contractually obligated and at the direction and authorization of [the school district] as legal owner, to enable the Police Defendants to recover and return District's stolen computer." Doc. #78, at 11. They maintain that, under these circumstances, no reasonable jury could find that their conduct was outrageous, extreme, utterly intolerable, or beyond all possible bounds of decency as required.<sup>12</sup>

In the Court's view, based on the evidence presented, a reasonable jury could find that the Absolute Defendants wrongfully intruded into Plaintiffs' activities "in such a way as to outrage or cause a person of ordinary sensibilities to suffer mental suffering, shame or humiliation." *Housh*, 165 Ohio St. 35, 133 N.E.2d 340, ¶ 2 of syl. As one court has explained, the tort at issue is "akin to a

---

<sup>12</sup> Citing the unpublished case of *Huntington Center Associates v. Schwartz, Warren & Ramirez*, No. 00AP-35, 2000 Ohio App. LEXIS 4388 (Ohio Ct. App. Sept. 26, 2000), the Absolute Defendants argue that the conduct alleged must be "so outrageous in character, and so extreme in degree, as to go beyond all possible bounds of decency, and to be regarded as atrocious, and utterly intolerable in a civilized community." *Id.* at \*15 (quoting *Haller v. Phillips*, 69 Ohio App.3d 574, 578, 591 N.E.2d 305 (Ohio Ct. App. 1990)). This quote from *Haller*, however, actually referred to the elements of the tort of intentional infliction of emotional distress. The court noted that this particular tort and the tort of invasion of privacy were subject to a "similar standard." *Haller*, 69 Ohio App.3d at 578, 591 N.E.2d at 307.

trespass in that it involves intrusion or prying into the plaintiff's private affairs. Examples would be *wiretapping*, [or] watching or photographing a person through windows of his residence." *Killilea v. Sears, Roebuck & Co.*, 27 Ohio App.3d 163, 166, 499 N.E.2d 1291 (Ohio Ct. App. 1985) (emphasis added).

Although the Absolute Defendants may have had a noble purpose, to assist the school district in recovering its stolen laptop, a reasonable jury could find that they crossed an impermissible boundary when they intercepted Plaintiffs' instant messages and webcam communications. A reasonable jury could also find that such conduct would cause a person of ordinary sensibilities to suffer shame and humiliation. For these reasons, the Court overrules the Absolute Defendants' Motion for Summary Judgment on this claim.

### **3. Springfield Defendants**

Ashworth and Lopez argue that they cannot be held liable for an invasion of privacy because they did not intercept Plaintiffs' communications or do anything to actively intrude on their privacy. In support of this argument, they cite to *Beard v. Akzona*, 517 F. Supp. 128 (E.D. Tenn. 1981), and *Fields v. Atchison, T. & S.F. Railway*, 985 F. Supp. 1308, 1312-13 (D. Kan. 1997), *withdrawn in part on other grounds on motion for reconsideration*, 5 F. Supp.2d 1160 (D. Kan. 1998). In each of those cases, the defendants did nothing more than listen to tapes of telephone conversations that had been illegally recorded by a third party. Defendants had nothing to do with the illegal interception. The courts held that these facts did not

give rise to a claim for intrusion upon seclusion because there was no evidence that, by simply listening to tapes, defendants had intentionally intruded on plaintiffs' solitude or seclusion. *See Beard*, 517 F. Supp. at 132; *Fields*, 985 F. Supp. at 1312-13.

One other case is quite instructive. In *Quigley v. Rosenthal*, 327 F.3d 1044 (10th Cir. 2003), the Aronsons made illegal tape recordings of their neighbors' cordless telephone conversations, and then filed a complaint with the Anti-Defamation League based on anti-Semitic statements and threats made during those phone conversations. The Anti-Defamation League held a press conference, and criminal charges were eventually filed against the Aronson's neighbors, the Quigleys. The Quigleys then filed a civil suit against the Anti-Defamation League and its attorney, alleging defamation, invasion of privacy, and violations of federal wiretapping laws. At trial, the jury found in favor of the Quigleys on a majority of the claims.

Defendants appealed. As to the invasion of privacy by intrusion claim, the Tenth Circuit held that the district court had erred in instructing the jury that it could find in favor of the Quigleys if they found either that the defendants had "intercepted" private telephone conversations or "used" the contents of those conversations. The court explained as follows:

Although it is clear that the interception of the Quigleys' telephone conversations would constitute an intentional intrusion on the Quigleys' seclusion or solitude, the issue raised by defendants is whether, as set forth in the district court's instructions, the "use" of

intercepted telephone conversations can also constitute such an intrusion. We conclude the answer to this question is "no." In particular, once the interception of the conversations was complete, any subsequent "use" of the conversations could not have resulted in any additional intrusion on the Quigleys' seclusion or solitude. Certainly, the "use" of such conversations might have resulted in another type of invasion of privacy, i.e., unreasonable publicity given to another's private life. But no such claim was asserted in this case. We therefore conclude that the district court committed plain error in instructing the jury on plaintiffs' invasion of privacy by intrusion claims, and that such error warrants a reversal of the judgment on those claims.

*Quigley*, 327 F.3d at 1073.

These cases indicate that, in order to be liable on a claim for "wrongful intrusion" invasion of privacy claim, the defendant must do something to actively intrude on the plaintiff's seclusion or privacy. Comment (b) to Restatement (Second) of Torts § 652B, discussing "wrongful intrusion" claims, states as follows:

The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff's room in a hotel or insists over the plaintiff's objection in entering his home. It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires. It may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents. The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined.

Restatement (Second) of Torts § 652B cmt. b (1977).

In this case, the Springfield Defendants had nothing to do with the interception of Plaintiffs' electronic communications. They simply "used" the evidence provided by the Absolute Defendants to trace the stolen laptop to Clements-Jeffrey and to arrest her for receiving stolen property. Granted, their "use" of the sexually explicit communications during the course of questioning her may have been unprofessional and entirely gratuitous, but, as in *Quigley*, such "use" did not result in any additional intrusion on the plaintiffs' seclusion or solitude. Based on the cases cited above, the Court concludes that the Springfield Defendants are entitled to summary judgment on this claim.

Ashworth and Lopez also argue that they are statutorily immune from damages under Ohio Revised Code § 2744.03(A)(6) because they were acting in the scope of their employment and because no reasonable jury could find that they acted with malice, in bad faith, or were wanton or reckless. Having determined that Defendants' conduct does not rise to the level of an actionable tort, the Court need not address this issue.

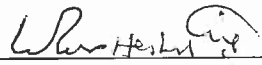
#### **IV. Conclusion**

For the reasons set forth above, the Court SUSTAINS the Springfield Defendants' Motion for Partial Summary Judgment (Doc. #70), but notes that Plaintiffs' § 1983 claim arising out of the warrantless search of Clements-Jeffrey's apartment remains pending.



Because there are genuine issues of material fact with respect to all claims asserted against the Absolute Defendants, the Court OVERRULES the Absolute Defendants' Motion for Summary Judgment (Doc. #78).

Date: August 22, 2011

  
WALTER HERBERT RICE  
UNITED STATES DISTRICT JUDGE

Copies to:

Counsel of record